



Office, Director of Information
Systems for Command, Control,
Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

18 Oct 01

SAIS-IOA

MEMORANDUM FOR UNITED STATES ARMY PUBLISHING AGENCY

SUBJECT: U.S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy

1. Enclosed is the Army Wireless LAN and Wireless PED Policy. Also enclosed is the request for publishing (Form 260), and limited staffing authority given by the Office of the Administrative Assistant to the Secretary of the Army (OAASA).
2. Integration of Wireless LANs and PEDs into Army networks and systems increases the risks of information compromise and network intrusions if not implemented in a secure manner. The recently discovered security vulnerabilities associated with the use of wireless devices necessitates the distribution of this policy immediately.
3. Requested action: Rapid Action Processing.
4. Desired distribution date: Immediate distribution via the USAPA website.
5. Expiration date: Two years after date of issue.

PETER M. CUVIELLO
Lieutenant General, GS
Director

3 Encls

1. Army Wireless LAN
and PED Policy
2. DA Form 260
3. Limited Staffing
Authority

SUBJECT: U. S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy.

1. Purpose.

This letter provides policy for the acquisition and use of wireless communication solutions and PEDs (data enabled cellular phones, two-way pagers, personal digital assistants (PDA), and handheld / laptop computers with wireless connectivity capabilities). This policy applies to the active Army, Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR).

2. Proponent and exception authority. The proponent of this letter is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4)(SAIS-ZA). The proponent has delegated exception authority to the director of Information Assurance (SAIS-IOA) for all matters pertaining to Army networks security.

3. References.

- a. Army Regulation 380-19: Information Systems Security, 27 Feb 1998.
- b. Army Regulation 25-1: Army Information Management, 15 Feb 2000.
- c. Army Regulation 380-53: Information Systems Security Monitoring, 29 Apr 1998.
- d. Army Regulation 5-12: Army Management of Electromagnetic Spectrum, 1 Oct 1997.
- e. Department of Defense Instruction 5200.40: DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 1997.
- f. Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (rev. 2), 31 Mar 2001.
- g. Department of Defense Directive 5000.1: Defense Acquisition System, 23 Oct 2000.

4. Explanation of abbreviations.

- a. 3DESTriple Data Encryption Standard
- b. AESAdvanced Encryption Standard
- c. AISAutomated Information System
- d. ARArmy Regulation

- e. ARNGUS.....Army National Guard of the United States
- f. CDMA.....Code Division Multiple Access
- g. COTSCommercial off the Shelf
- h. DAADesignated Approval Authority
- i. DISC4Director of Information Systems, Command, Control,
Communications, and Computers
- j. DITSCAP.....Defense Information Technology Security
Certification and Accreditation Process
- k. DoDDepartment of Defense
- l. DoDDDepartment of Defense Directive
- m. DoDIDepartment of Defense Instruction
- n. DoDIIS.....Department of Defense Intelligence Information
System
- o. ESSIDExtended Service Set Identifier
- p. FIPSFederal Information Processing Standards
- q. GSMGlobal System for Mobile Communications
- r. IEEEInstitute for Electrical and Electronic Engineers
- s. I&AIdentification and Authentication
- t. IDSIntrusion Detection System
- u. LANLocal Area Network
- v. MACMedia Access Control
- w. MCEBMilitary Communications Electronics Board
- x. NISTNational Institute for Standards and Technology
- y. NSANational Security Agency
- z. PANPersonal Area Network

SUBJECT: U. S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy.

- aa. PCPersonal Computer
- ab. PEDPortable Electronic Device
- ac. PDAPersonal Digital Assistant
- ad. PINPersonal Identification Number
- ae. PKIPublic Key Infrastructure
- af. SCISensitive Compartmented Information
- ag. SCIFSensitive Compartmented Information Facility
- ah. TDMA.....Time Division Multiple Access
- ai. TLATop Level Architecture
- aj. USARUnited States Army Reserve
- ak. VPNVirtual Private Network
- al. WAPWireless Access Protocol
- am. WEPWired Equivalent Privacy

5. Responsibilities.

a. Currently fielded wireless LAN and PED technologies that are not in compliance with this policy must have migrations plans developed to ensure the systems will meet the requirements of this policy. For non-compliant wireless implementations, the Designated Approval Authority (DAA) is responsible for approving and maintaining these migration plans as part of their acceptable level of risk determination. All Army activities considering wireless LAN and PED technologies must adhere to the requirements outlined below.

(1) Pilot and fielded wireless LANs and PEDs with LAN connectivity must meet the same certification and accreditation security requirements as wired LAN automated information systems (AIS) per AR 380-19 (until superseded by AR 25-1A), AR 380-53, AR 25-1, and DoDI 5200.40. Pilot projects must consider these requirements during the development of the system.

(2) Wireless solutions will be engineered to preclude backdoors into the Army's LANs. Backdoors could be caused by either unprotected transmissions or unprotected

PEDs entering a network. Consideration of both factors must be evaluated in the design of a wireless solution.

(3) Commercial off the shelf (COTS) products typically arrive with factory default settings that may not offer appropriate security. Wireless equipment that connects to a LAN will be configured for acceptable LAN security options.

(4) IEEE 802.11, the industry standard for wireless LAN equipment, is the standard to consider when acquiring wireless LANs.

(5) Where wireless LANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information intercept / monitoring and network intrusion.

(6) Ensure that a user cannot enter a wireless LAN without strong authentication. As a minimum, strong authentication will include extended service set identification (ESSID) and a media access control (MAC) address identification with an integrity lock. MAC address resolution alone does not qualify as strong authentication.

(a) ESSID is a common access number / code that is applied to a wireless access point during configuration and with associated wireless network interface cards so access points can identify an authorized group of mobile units.

(b) The MAC address is a unique numeric identifier that is programmed into a wireless network interface card by the manufacturer. Some manufacturers allow this identifier to be reprogrammed by the user, therefore, it must be assumed that the MAC address can be copied electronically (spoofed) and used to gain unauthorized access to an AIS.

(7) Wireless LAN and PED solutions must use the full implementation of a National Institute for Standards and Technology (NIST) Federal Information Processing Standards (FIPS) publication 140-1 (or 140-2 when available) level 1 validated crypto module using Triple data encryption standard (3DES), or the new Advanced Encryption Standard (AES) for those situations requiring protection of sensitive information. Wireless LANs transmitting unclassified data that is not of a sensitive nature will require encryption using level 1 NIST FIPS 140-1 or 140-2 validated crypto modules if they are connected to LANs that handle sensitive information. NSA approved, type 1 encryption must be used for any situation requiring protection of classified information.

(a) The Wired Equivalent Privacy (WEP) security protocol built into the 802.11 standards for wireless LANs does not use a FIPS-validated crypto module and has been found by the cryptographic community to have fundamental flaws. Those implementing wireless LANs must investigate additional security measures for data confidentiality and network intrusion protection, such as the use of virtual private network (VPN) gateways that use FIPS-validated crypto modules.

(b) A more secure encryption for the 802.11 standards is currently being evaluated, but it is not known if a software / firmware upgrade to the more secure encryption will be possible or if the new encryption scheme will be FIPS-validated.

(c) Those planning wireless LAN solutions must consider that migration to more secure wireless LAN technologies could mean costly replacement of equipment.

(8) As technology advances, approved anti-virus software for PEDs will be available. To ensure consistent levels of protection required against viruses, it is

SUBJECT: U. S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy.

important to maintain up-to-date signature files that are used to profile and identify viruses, worms, and malicious code. The network infrastructure must accommodate anti-virus software updates for all PEDs supporting desktops and servers.

(9) PEDs, other than approved laptop computers, will not be used for classified information processing. PEDs do not currently provide adequate security mechanisms to protect classified data from compromise.

(10) PEDs with wireless communication capabilities will not be permitted inside a sensitive compartmented information facility (SCIF) unless, as a minimum, the device's infrared port has been completely covered by an opaque tape and / or it's antenna has been removed / physically disabled; however, the agency in charge of any given SCIF is the authority for the procedures to move PEDs in or out of their facilities (ref. Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, Chapter 15 (Portable Electronic Devices), and AR 380-19, paragraph 2-13). The various wireless and wired interconnection capabilities of PEDs present significant risk of compromise of classified information over an unclassified medium.

(11) In no instance shall a PED without strong identification and authentication (I&A, i.e. login and password) be used to store, process, or transmit official Army information. PEDs without strong I&A built in or added to the system should only be used for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.

(12) The DoD Public Key Infrastructure (PKI) and digital certificates will be used to the greatest extent possible to support security solutions for user identification and authentication, data confidentiality (using FIPS-validated crypto modules), and non-repudiation when using PEDs for wireless communications. Security solutions using digital certificates must comply with DoD PKI requirements. When external certificate authorities are necessary, issuance of certificates, plans for key escrow, and revocation of user certificates must be documented.

(13) Personal area networks (PAN) (including Bluetooth) will not be utilized for transmitting sensitive information unless the data is encrypted with a FIPS-validated crypto module or the area in which the PAN devices communicate (within approximately 30 ft) is within a physically controlled and radio frequency-secured area.

(14) Web-enabled PEDs that rely on wireless access protocol (WAP) and / or use commercial wireless network providers are at risk for information compromise. Data will not be transmitted in this situation unless it can be ensured that data is encrypted end-to-end using a FIPS-validated crypto module. The WAP standard is evolving to support data confidentiality requirements through the use of PKI digital certificates and by allowing customers to run their own WAP gateways for secure, direct connections to web-based resources.

(15) WAP gateways will be installed in the Top Level Architecture (TLA) of Army installation networks so that wireless access to web-servers may be properly controlled and monitored by firewalls and intrusion detection systems (IDS).

(16) The use of any wireless device, including commercial unlicensed devices, must be coordinated with the local Army frequency manager prior to purchase. Use of

wireless devices may not be approved for use in another country, since each country allocates its frequency resources differently.

(17) All wireless devices procured with army funds must be certified for spectrum supportability through the Military Communications Electronics Board (MCEB) per DoDD 5000.1 and AR 5-12. Spectrum supportability request should be submitted to the US Army C-E Services Office.

(18) All users being issued a PED must be provided security awareness training regarding the physical and information security vulnerabilities of the device.

b. Army commands and activities whose members use PEDs that synchronize with desktop computers on Army networks will adopt the following security measures and write them into command AIS security policies, security awareness and training, and network user agreements:

- (1) Only use applications that are approved by the local DAA.
- (2) PEDs will only be connected to unclassified computers.
- (3) Passwords, combinations, personal identification numbers (PIN) and classified information will not be stored on PEDs.
- (4) Do not use a PEDs remote connectivity features while it is physically connected to a desktop PC, particularly a networked PC, or otherwise connected to the network.

6. Considerations before acquiring and using wireless LANs and PEDs.

a. A significant security factor associated with the proper use of wireless technologies and, in particular, PEDs is the acknowledgement by the user that the PED is, in fact, functioning in the same capacity as a standard PC or workstation; therefore, it is subject to the same regulations. Reinforcing the standard information security training and discussion of the Army's Defense In Depth program as part of this training can help to raise user awareness of the vulnerabilities associated with these systems. The Defense In Depth Program is a security strategy endorsed by the Army as a means to counter security vulnerabilities.

b. The following characteristics/parameters of wireless solutions must be considered prior to the use of any wireless solution:

(1) Wireless solutions may create backdoors into Army LANs. If a device receives information via a wireless technology and that device allows that information to be placed directly into the LAN at the workstation level, then all perimeter and host-based security devices have been bypassed.

(2) Wireless LANs are susceptible to interference, interception, and can be jammed.

(3) Currently, there are three major wireless telephone transmission-multiplexing techniques in use by commercial wireless service providers in the U.S. (CDMA, TDMA, and GSM). Each transmission standard is incompatible with the others. Equipment operating using one standard cannot communicate with equipment using a different standard.

**SUBJECT: U. S. Army Wireless Local Area Networks (LAN) and Wireless
Portable Electronic Devices (PED) Policy.**

Distribution:

HQDA (SASA)
HQDA (DACS-ZA)
HQDA (DACS-ZB)
HQDA (SACW)
HQDA (SAFM-AOA)
HQDA (SAILE)
HQDA (SAMR)
HQDA (SARD)
HQDA (SAGC)
HQDA (SAAA-PP)
HQDA (DACS-ZD)
HQDA (SAIS-ZA)
HQDA (SAIG-ZA)
HQDA (SAAG-ZA)
HQDA (SALL)
HQDA (SAPA)
HQDA (SADBU)
HQDA (DAMI-ZA)
HQDA (DALO-ZA)
HQDA (DAMO-ZA)
HQDA (DAPE-ZA)
HQDA (DAEN-ZA)
HQDA (DASG-ZA)
HQDA (NGB-ZA)
HQDA (DAAR-ZA)
HQDA (DAJA-ZA)
HQDA (DACH-ZA)
HQDA (DAIM-ZA)
HQDA (JDIM-RM)

COMMANDING GENERAL

U.S. ARMY, EUROPE AND SEVENTH ARMY

COMMANDERS

EIGHTH U.S. ARMY

U.S. ARMY FORCES COMMAND

U.S. ARMY MATERIEL COMMAND

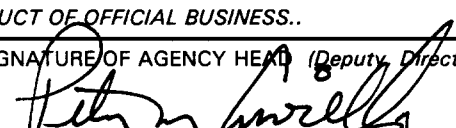
U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. SPECIAL OPERATIONS COMMAND

U.S. ARMY PACIFIC

MILITARY TRAFFIC MANAGEMENT COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY MEDICAL COMMAND
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY SOUTH
U.S. ARMY RECRUITING COMMAND
U.S. ARMY COMMUNITY AND FAMILY SUPPORT CENTER

REQUEST FOR PRINTING OF PUBLICATION		DATE 09/28/2001
For use of this form, see AR 25-30; the proponent agency is OAASA.		
TO: (Include ZIP Code) Attn: JDHQSVPAP-D 2461 Eisenhower Avenue Alexandria, VA 22331-0302	FROM: (Originating Agency) HQDA (SAIS-IOA)	
	PERSON TO CONTACT Ms. Melissa Hicks	TELEPHONE/AUTOVON NO. 703-604-7548
PART I - COMPLETED BY ORIGINATING AGENCY		
1. TYPE AND TITLE OF PUBLICATION (On Confidential or higher classified publications, indicate the title which can be listed in index (DA Pamphlet 310-1)) HQDA Letter, U.S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy.		
2. JUSTIFICATION (Indicate why publication is needed, such as statutory requirement, DOD Directive, etc.) REQUIRED STATEMENTS/ CLEARANCES, INFORMATION, AND SPECIAL REQUESTS (Use reverse side and plain paper for additional space if necessary) Without approved security processes in place, wireless solutions will expose Army sensitive information to interception and will create backdoors into Army Networks. The purpose of this message is to disseminate guidance and policy for the aquisition and use of wireless communications solutions and portable electronic devices (data enabled cellular phones, two-way pagers, personal digital assistants (PDA), and handheld / laptop computers with wireless connectivity capabilities). This HQDA letter is for "RAPID ACTION PROCESSING".		
3. RELATED PUBLICATIONS NONE	4. PUBLICATIONS TO BE SUPERSEDED (DA publications (including interim changes), forms, and requirement control symbols (RCSs)) NONE	
5. COPYRIGHT MATERIAL		
a. INCLUDED IN MANUSCRIPT (If "YES" copy of copyright release must be attached) <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	b. HELD BY (Name and address, include ZIP Code, of copyright owner)	
6. DISTRIBUTION RESTRICTION (Publication contains material that would restrict distribution) <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	7. SALE BY SUPERINTENDENT OF DOCUMENTS <input type="checkbox"/> MAY BE SOLD <input checked="" type="checkbox"/> NOT TO BE SOLD	
8. RECOMMENDED DISTRIBUTION (Include statement as to whether or not distribution to National Guard and USAR is required) Distribution via the USAPA website in accordance with instructions given by the Office of the Aministrative Assistant to the Secretary of the Army. This letter applies to the active Army, the Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR).		
THIS PUBLICATION, FOR WHICH PRINTING IS REQUESTED, DOES NOT UNNECESSARILY DUPLICATE EXISTING PUBLICATIONS AND IS ESSENTIAL TO THE EFFECTIVE, EFFICIENT, AND ECONOMICAL CONDUCT OF OFFICIAL BUSINESS..		
TYPED NAME AND GRADE OF AGENCY HEAD (Deputy, Director, or Division Chief) Peter M. CuvIELLO, LTG, GS, Director	SIGNATURE OF AGENCY HEAD (Deputy, Director, or Division Chief) 	

PART II - CONCURRENCES

LIST AGENCY AND NAME AND GRADE OF CONCURRING OFFICER

US Army Materiel Command (AMC), Ms. Mary Carroll, IAPM

US Army Forces Command (FORSCOM), Mr. Don Labonte, IAPM

US Army Training and Doctrine Command (TRADOC), Ms. Mary Campbell, IAPM

US Army Special Operations Command (USASOC), Mr. Jorge E. Rios Calero, Chief- IA

US Army Corps of Engineers (USACE), repeated attempts, no response from IAPM, concurrence assumed

US Army Medical Command (MEDCOM), Mr. Ross J. Roberts, IAPM

US Army Pacific Command (USARPAC), Mr. Paul A. Scheftel, IAPM

US Army Military District of Washington (MDW), CW5 Richard R. Coombe, IAMP

US Army South (USARSO), repeated attempts, no response from IAPM, concurrence assumed

US Army Intelligence and Security Command (INSCOM), Byron Renner, IAPM

PART III - APPROVING AUTHORITY *(To be used by general staff or higher level agencies when submitted thereto for approval)*

APPROVED FOR PUBLICATION

PART IV - PUBLICATION CONTROL ACTION

APPROVED IN ACCORDANCE WITH AR 310-3.

DATE

TYPED NAME AND GRADE

SIGNATURE

PART V - REQUIREMENT CONTROL ACTION

APPROVED IN ACCORDANCE WITH AR 335-15. REQUIREMENT CONTROL SYMBOL ASSIGNED: _____

DATE

TYPED NAME AND GRADE

SIGNATURE

CONTINUATION/REMARKS

Concurrences continued:

US Army Criminal Investigation Command (USACIDC), Mr. Angel L. Gonzalez, IANM

US Army Recruiting Command (USAREC), Mr. John W. Teegarden, IANM

US Army Community and Family Support Center (USACFSC), Mr. Howard Haney, IAPM

US Army Security Assistance Command (USASAC), Mr. Ricky Tanna

Eighth US Army (EUSA), Mr. Gene Nittinger, IAPM

Military Traffic Management Command (MTMC), Ms. Kimberly Quinn, IAPM

ASA(FM&C), LTC Brian Cummings

ODSCINT DAMI-POD, Mr. Thomas O'Brien

ODISC4 SAIS-IMC, Ms. Arlene Dukanauskas

ODISC4 SAIS-IAS, LTC(P) Thaddeus Dmuchowski

OTJAG, MAJ Carrie Ricci-Smith (no legal objection)

OGC, Ms. Susan Tigner (no legal objection)

NISA-SR, SFC William B. Cole

ODCSPER, LTC Robert Grunewald

ODCSOPS, no comments, no replies, concurrence assumed

PEO STAMIS, Mr. Greg Seitz, IAPM

Foster, Noel Mr DISC4/SYTEX

From: Hicks, Melissa Ms DISC4
Sent: Wednesday, June 06, 2001 11:19 AM
To: Foster, Noel Mr DISC4/SYTEX
Cc: Jerome, Harold W Mr PPO; Krist, Kirk M COL DISC4; Robison, Gary A Mr DISC4; Lundgren, LeRoy Mr DISC4/Sytex
Subject: FW: Wireless LAN and PED guidance
Importance: High

Noel,

I spoke with Hal Jerome today. He said that this email you received from Tony Tatum provides the authorization for limited staffing.

Mr. Tatum lists the organizations for this coordination effort. We must attach this email to the FORM 260 that we send to USAPA.

Melissa

-----Original Message-----

From: Jerome, Harold W Mr PPO
Sent: Wednesday, June 06, 2001 11:10 AM
To: Hicks, Melissa Ms DISC4
Subject: FW: Wireless LAN and PED guidance
Importance: High

Melissa, per our conversation, FYI. Hal

-----Original Message-----

From: Tatum, Anthony W Mr PPO
Sent: Wednesday, May 30, 2001 12:42 PM
To: Foster, Noel Mr DISC4/SYTEX
Cc: Jerome, Harold W Mr PPO; Richwine, Robert J Mr PPO; Czekner, John Mr USAPA; Dukauskas, Arlene M Ms DISC4; Scullen, Tom M Mr HQDA-SSA
Subject: RE: Wireless LAN and PED guidance

The Admin Assistant has previously put out a memo to curtail the issuance of "policy" via E-Messages due to the fact that the policy stated in several of those E-Messages never got revised into the official regulation. E-Messages are not numbered or indexed as Army Regulations, therefore, there is currently no life cycle management of policy issued via E-Messages.

Just a reminder, Army Policy must be authenticated by the Secretary of the Army prior to release.

Recommend formatting the language in your proposed message into a numbered HQDA Letter and submitting for release as an "official policy" document.

Hal Jerome or Bob Richwine of our office will gladly grant you limited staffing authority. I suspect you will need to - at a minimum- staff with ASA(FM&C) DCSINT, MACOMs using PED, and OTJAG.

USAPA (John Czekner) will gladly work with you to expedite posting of the HQDA Letter on the Army Pubs Web Site. USAPA has been pretty good at getting the HQDA letters out about as quick as you can get an E-Message put out.

A last thought, you could send out a message that alerts the field that new policy is expected to be forthcoming, but it can't "direct" action in the way of Army Policy since it is not authenticated by the Secretary of the Army.

Hope this helps

Tony Tatum

Policy and Plans Office
Office of the Administrative Assistant
to The Secretary of the Army
(703) 697-3067 DSN 227-3067

-----Original Message-----

From: Foster, Noel Mr DISC4/SYTEX
Sent: Wednesday, May 30, 2001 11:07 AM
To: Tatum, Anthony W Mr PPO
Subject: Wireless LAN and PED guidance

Mr. Tatum,

Ms. Arlene Dukanauskas advised that I should include you in the staffing of this draft guidance. This is a security issue and it is critical that this be disseminated as soon as possible. Please review the message and respond with your concurrence / non-concurrence. Thank you.

V/R

Mr. Noel Foster (SYTEX, INC)
Information Assurance Office, ODISC4
Department of the Army
PH: 703-601-0740 DSN: 329-0740
FAX: 703-607-5599 DSN: 327-5599
<mailto:Noel.Foster@hqda.army.mil>

<< File: wirelessfinal4.doc >>